IN THE SPECIFICATION:

Please replace paragraph [0039] with the following amended paragraph:

[0039] In one embodiment, the capacity manager 120 is at least a component of a Capacity on Demand function provided on machines from International Business Machines, Inc. One such machine is the eServer iSeries® computer. By way of illustration only, the capacity manager 120 and user interface 118 are shown as components of an operating system 122. Examples of the operating system 122 include an IBM OS/400® operating system, an AIX® operating system, a UNIX® operating system, a Microsoft Windows® operating system, and the like. However, the illustrated representation is merely one example of a particular software architecture, and not limiting of the invention. OS/400® and AIX®, are registered trademarks of International Business Machines, Inc., and Microsoft Windows® is a registered trademark of Microsoft, Inc.

Please replace paragraph [0055] with the following amended paragraph:

[0055] The code validation algorithm 124 then sends to the smart chip 130 the encrypted MAC 204 that was included with the disablement code (step 506). Upon receipt, the smart chip 130 decrypts the MAC 204 using its unique key 134 (step 508), which is presumably the same key as was used to encrypt the MAC 204. This decryption yields a decrypted MAC, referred to herein as the smart chip MAC 514. If the keys are not the same, the decryption will be unsuccessful (step 510). An unsuccessful decryption may result in the sequence 414 returning an error (step 512) if parity checking is implemented and the parity is wrong. Alternatively, the validation software determines that the decryption was not successful by comparing or using the keys (i.e., the MAC 204 and the smart chip MAC 514) and determining that they are different. Persons skilled in the art will recognize other embodiments. In any case, if the keys are the same, the decryption is successful and yields the smart chip MAC 514, which will be the same as the MAC 202 generated by the MAC generator algorithm 125 in FIGURE 2.

Please replace paragraph [0056] with the following amended paragraph:

[0056] To verify that both are using the same MAC, the code validation algorithm 124 and the smart chip 130 exchange encrypted data, each using its own copy of the MAC as encryption key. It is noted that any variety of exchanges is contemplated and the following is merely illustrative. In one embodiment, the exchange is initiated by the code validation algorithm 124, which generates a random value (step 513), encrypts the value using the validation MAC 504 as a key (step 515), and then sends the encrypted value to the smart chip 130 (step 516). Upon receipt, the smart chip 130 decrypts the random value using the smart chip MAC 514 as decryption key (step 518). The smart chip 130 then sends the decrypted random value to the code validation program 124 (step 520). Upon receipt, the code validation algorithm 124 compares the received decrypted random value to the original random value (step 522). If the values are the same (step 524), it is confirmed that the disablement code 115 has been input to the appropriate system, with respect to which the disablement code 115 is unique. If the values are the same, an indication of the success may be returned by the sequence 414 (step 528), and the code validation algorithm 124 disables the On/Off Capacity feature (steps 416 and 418 of FIGURE 4); otherwise, an error may be returned (step 526).

Please replace the Abstract with the following amended Abstract and note that a clean copy is attached:

Method, apparatus and article of manufacture for disabling on-demand access to computerized resources on a computerized apparatus. The method comprises receiving a disablement code; validating the disablement code; and disabling an on-demand resource if the validating is successful, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus. Another embodiment includes receiving a disablement code comprising encrypted data, validating the disablement code, disabling at least one on-demand

resource if the validating is successful. The validating includes generating a first key using system information unique to the computerized apparatus; decrypting the encrypted data using a second key to produce decrypted data; encrypting a value to produce an encrypted value; decrypting the encrypted value to produce a decrypted value; and comparing the value to the decrypted value.